



Apache ModSecurity

Stefan Schindewolf

Provadis School of International Management and Technology

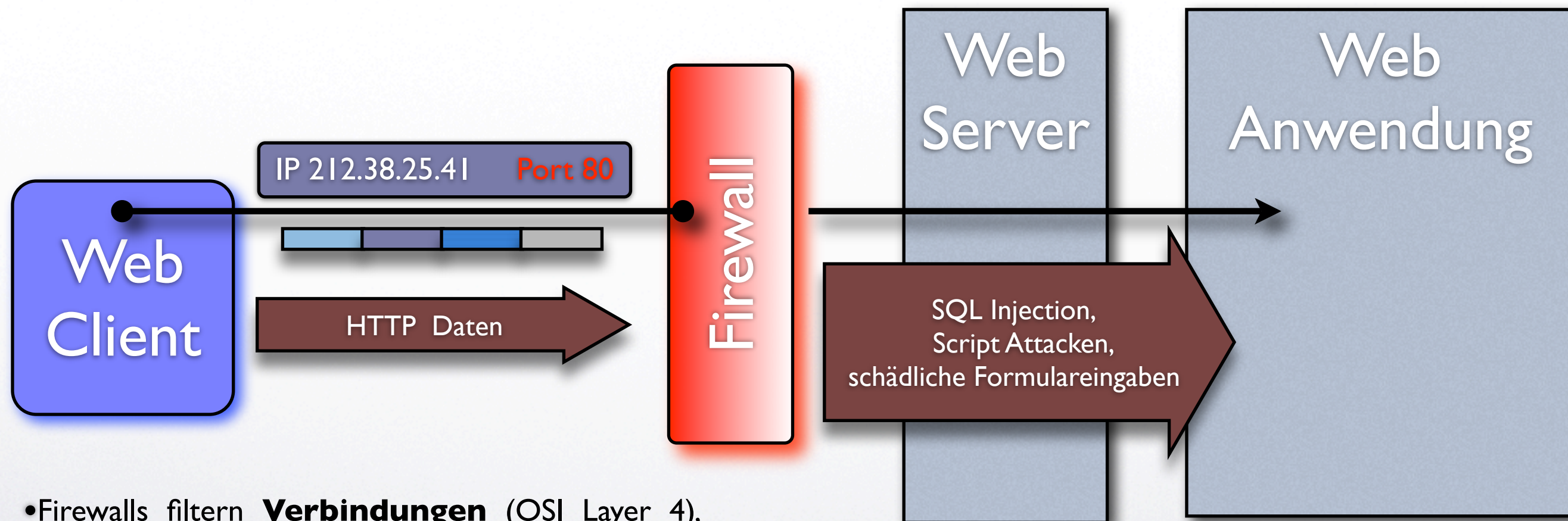


Was ist ModSecurity?

- Web Application Firewall für Apache
- Oder: Apache Modul zum Erkennen und Verhindern von Einbrüchen



Was ist eine Firewall?



- Firewalls filtern **Verbindungen** (OSI Layer 4), jedoch **nicht** die **Inhalte** der verschickten Daten
- Ergo: kein Schutz gegen Angriffe auf die Anwendung (OSI Application Layer 7)

- Angriffe auf Layer 7 machen im Internet ca. 70% aller Attacken aus (Quelle: modsecurity.org)



Application Firewall

- Arbeitet auf OSI Layer 7 (Application Layer)
- Untersucht die Inhalte der verschickten Daten
 - ➔ HTTP/S Protokoll (Formularfelder, Transaktionen, hochgeladene Dateien)
 - ➔ beherrscht aber auch Applikationsdatenverkehr, z.B. SQL Überwachung von SQL-Verbindungen, IP-Telephonie, Filesharing, etc.
- Filtert schadhafte Eingaben in Formularen, Dateianhängen, SQL-Befehlen, Programmcode, etc.
- Blockiert Angriffe, *bevor* sie Schaden anrichten (Unterschied zu Intrusion Detection) oder leitet Angreifer einfach um (Honeypot Redirecting)



ModSecurity Features

1. Entdecken nicht protokollgerechter HTTP/S Requests

2. Web Attacken
Sicherung

- SQL Injection
- Cross-Site Scripting (XSS)
- Betriebssystem Befehle
- Quellcode Injizierung
- LDAP Injection
- SSI Injection
- Buffer overflows

3. Entdecken automatisierter Attacken

- SPAM
- Crawler
- Bots

4. Entdecken von Trojaner Datenverkehr

- Erkennen installierter Trojaner
- Integration von Virensclannern

5. Zurückhalten von Fehlermeldungen an Client (keine Informationen für Angreifer)



Einfache Konfiguration

```
SecFilterEngine On
```

Einschalten von ModSecurity

```
# URL-Validierung aktivieren  
SecFilterCheckURLEncoding On
```

```
# Unicode-Validierung aktivieren  
SecFilterCheckUnicodeEncoding On
```

```
# HTTP-POST-Daten verarbeiten  
SecFilterScanPOST On
```

```
# Standard-Aktion für zutreffende Filterregeln  
SecFilterDefaultAction "deny,log,status:403"
```

Rückmeldung an den Client

```
# Filterregeln aus mod-security.d einbinden  
Include /etc/mod-security.d/[^.#]*
```

Verweis auf Filterregeln



einfache Filterregeln

- Format von Filterregeln: `SecFilter AUSDRUCK [AKTION]`
- Beispiel: `SecFilter /bin/sh deny`

Schlüsselwörter
reguläre Ausdrücke

Aktionen:

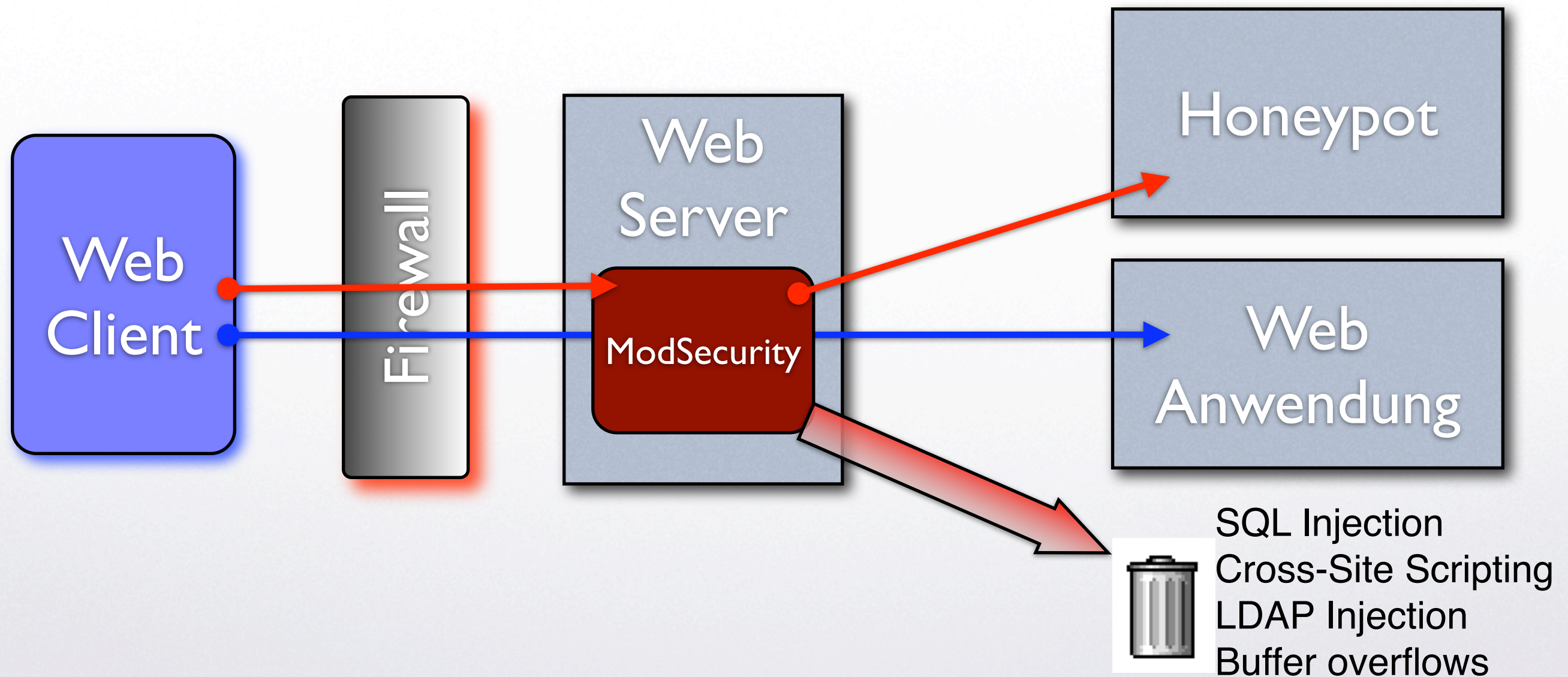
deny, pass, redirect, ...

Request:

`/index.php?exec=/bin/sh%20/var/www/upload/x.sh`



Advanced Filtering





ModSecurity.org Facts

- Freie Software, quelloffen (www.modsecurity.org)
- Ivan Ristic entwickelt ModSecurity seit 4 Jahren
- Als kommerzielles Produkt mit professionellem Support verfügbar bei Breach Security Inc.
-



Quellen und Links

- Homepage: <http://www.modsecurity.org>
- <http://www.heise.de/security/artikel/69070>



Ausblick

- Entdecken von Korrelationen im Datenstrom zur Detektion von:
 - Denial of Service
 - Brute Force
 - Test- und Erkundungsangriffen
- Analyse von SOAP Requests
- Entwerfen von Signaturen für Standardattacken